United States District Court

EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

UNITED STATES OF AMERICA	§	
	§	4:16-CR-111
v.	§	(Judge Mazzant/Judge Nowak)
	§	
JOSE VICTOR HERNANDEZ-CUELLAR		

MEMORANDUM ADOPTING
RECOMMENDATION OF UNITED STATES MAGISTRATE JUDGE

Came on for consideration the report of the United States Magistrate Judge in this action, this matter having been heretofore referred to the Magistrate Judge pursuant to 28 U.S.C. § 636. On May 1, 2017, the report of the Magistrate Judge (Dkt. #47) was entered containing proposed findings of fact and recommendations that Defendant Jose Victor Hernandez-Cuellar's Motion to Suppress Evidence (Dkt. #25), Motion for Continuance of Suppression Hearing (Dkt. #40), and Opposed Motion Requesting Evidentiary Hearing (Dkt. #41) each be denied. Having received the report of the Magistrate Judge (Dkt. #47), and having considered Defendant's timely filed objections (Dkt. #49), and the Government's Response thereto (Dkt. #50), the Court is of the opinion that the recommendation of the Magistrate Judge is correct and the Motion to Suppress, Motion for Continuance, and Motion for Evidentiary Hearing each should be **DENIED**.

RELEVANT BACKGROUND

The Government's search and seizure of information from Defendant's computer and the subsequent search of his home form the basis of the present evidentiary dispute (*see generally* Dkt. #25; Dkt. #38; Dkts. #40-41; Dkt. #47). The Magistrate Judge sets out the facts of this case in further detail, and the Court need not repeat them here in their entirety (*see* Dkt. #47 at 1-5). Accordingly, the Court sets forth herein only those facts pertinent to Defendant's objections.

Defendant was indicted on September 7, 2016, for violation of 18 U.S.C. § 2251(a), (e) (Production of Child Pornography) (Dkt. #11). The Government's charges against Defendant arose following search of his home and seizure of evidence pursuant to a warrant issued by a United States Magistrate Judge in the Eastern District of Texas ("Residential Warrant") (*see* Dkt. #25, Exhibit 1). The Residential Warrant authorized search of Defendant's home (2201 Rockbrook Dr., Apartment 1131, Lewisville, Texas, 75067) based upon an affidavit provided by FBI Special Agent Christopher W. Thompson (Dkt. #25, Exhibit 1, Affidavit) ("Thompson Affidavit"). The Thompson Affidavit provides Thompson's credentials, explains Thompson's bases for probable cause to search Defendant's home and seize evidence therein, and describes the FBI's background investigation of a website (and its users) called "Playpen" or "Website A" (Thompson Affidavit at 11-20). Specifically, the Thompson Affidavit details the investigation of user "zapatero5" and the FBI's discovery of Defendant's access of Website A under such username (Thompson Affidavit at 20-23).

According to the Thompson Affidavit, "law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia" conducted an investigation of user zapatero5 (Thompson Affidavit at 14). More specifically, a United States Magistrate Judge in the Eastern District of Virginia ("Eastern District of Virginia Magistrate") issued the order (warrant) referenced in the Thompson Affidavit. This warrant authorized the search of computers, including Defendant's, accessing Website A's server (at a time when the server was located in the Eastern District of Virginia) through a set of computer instructions the FBI installed on the server called a "Network Investigative Technique" or "NIT" (Dkt. 25, Exhibit 2) ("NIT Warrant").

Defendant challenges the Residential Warrant only to the extent it relies upon the NIT Warrant as a basis for probable cause; Defendant concedes that, if the Court finds the NIT Warrant valid and legal, then the Residential Warrant would be facially valid, as well (Dkt. #46 at 3).

The NIT Warrant includes two attachments specifying the "[p]lace to be searched" (Attachment A) and the "[i]nformation to be seized" (Attachment B). Attachment A provides in whole as follows:

> This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.
> The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL - upf45jv3bziuctml.onion - which will be located at a government facility in the Eastern District of Virginia.
> The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password. The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.

(NIT Warrant, Attachment A). Attachment B describes the information to be seized as evidence of violations of various criminal statutes proscribing the use, distribution, or access of child pornography, namely the following:

> From any "activating" computer described in Attachment A:
> l . the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
> 2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other "activating" computers, that will be sent with and collected by the NIT;
> 3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
> 4. information about whether the NIT has already been delivered to the "activating" computer;
> 5. the "activating" computer's Host Name;
> 6. the "activating" computer's active operating system username; and
> 7. the "activating" computer's media access control ("MAC") address;

(NIT Warrant, Attachment B). The NIT Warrant, which expressly incorporates Attachments A and B, authorized the search "of computers that access [Website A]." The NIT Warrant was based upon an affidavit provided by FBI Special Agent Douglas Macfarlane (Dkt. #25, Exhibit 2, Affidavit) ("Macfarlane Affidavit"); the Macfarlane Affidavit provides Macfarlane's credentials and, *inter alia*, explains the function of the NIT. The Magistrate Judge summarizes the Macfarlane Affidavit's explanation as follows:

> The NIT "[was] designed to cause the [activating] computer to deliver to a computer known to or controlled by the government data that would help identify the computer, its locations, other information about the computer, and the user of the computer accessing 'Website A'" . . . . Specifically, the NIT would cause activating computers to send to the Government-controlled computer the seven pieces of information identified in Attachment B to the NIT Warrant . . . .

(Dkt. #47 at 3). Sometime between December 14, 2014, and March 5, 2015, the NIT collected the information described by Attachment B from a computer accessing Website A's server with the username zapatero5 (Thompson Affidavit at 20). The information included an IP address, which the FBI determined "was operated by the Internet Service Provider . . . Time Warner Cable" (Thompson Affidavit at 22). The FBI procured "an administrate subpoena/summons" and served it on Time Warner Cable in March 2015 "requesting information related to the user who was assigned the [identified] IP address" (Thompson Affidavit at 22). The information Time Warner Cable provided indicated the computer associated with the identified IP address was located at Defendant's home (Thompson Affidavit at 22-23). Subsequently, on November 6, 2015 (one day after the Residential Warrant issued), the FBI executed the Residential Warrant, seizing "incriminating statements" and Defendant's "personal computers and other digital devices" at his home (Dkt. #25 at 4).

Defendant filed the instant Motion to Suppress on December 30, 2016, seeking to suppress "all evidence, including statements, computers and digital images, seized from [Defendant] on or

about November 6, 11, [sic] 2015 and on various dates in 2016" collected pursuant to the Residential Warrant (Dkt. #25 at 1). The Government filed its Response to Defendant's Motion to Suppress on March 2, 2017 (Dkt. #38), and the Court set the matter for hearing ("Hearing") on March 14, 2017 (Dkt. #39). On March 10, 2017, Defendant filed the Motion for Continuance (Dkt. #40) and the Motion for Evidentiary Hearing (Dkt. #41). The Court held a Hearing on March 14, 2017 (Dkt. #45) related to the Motions, and the transcript of Hearing was filed April 26, 2017 (Dkt. #46). The Magistrate Judge entered a report and recommendation on May 1, 2017, recommending that the Court deny each of Defendant's Motion to Suppress, Motion for Continuance, and Motion for Evidentiary Hearing (Dkt. #47). On May 11, 2017, Defendant filed objections to the report and recommendation (Dkt. #49), and on May 17, 2017, the Government filed its Response to Defendant's objections (Dkt. #50).

DEFENDANT'S OBJECTIONS

A party who files timely written objections to a magistrate judge's report and recommendation is entitled to a de novo review of those findings or recommendations to which the party specifically objects. 28 U.S.C. § 636(b)(1)(C); Fed. R. Civ. P. 72(b)(2)-(3). The Magistrate Judge's report found as follows: (1) Defendant's Motion for Continuance should be denied as moot; (2) the NIT Warrant sufficiently particularized the "place to be searched" and the "items to be seized"; (3) the NIT Warrant issued in violation of Federal Rule of Criminal Procedure 41(b) and 28 U.S.C. § 636; and (4) the violation of Rule 41(b) and/or § 636 did not warrant suppression (Dkt. #47). In particular, the Magistrate Judge found the violation of Rule 41(b) and § 636 was technical—not fundamental or of constitutional dimension—and did not prejudice Defendant. Further, the Magistrate Judge found the good-faith exception to the exclusionary rule applied such that suppression would be inappropriate. The Magistrate Judge accordingly

concluded Defendant's Motion to Suppress and Motion for Evidentiary Hearing each should be denied (Dkt. #47). Defendant objects to the second finding, regarding the NIT Warrant's particularity, the fourth finding, regarding the nature of the violation of Rule 41(b) and § 636, and the finding regarding the applicability of the good-faith exception (Dkt. #49). Defendant also objects, as a result, to the Magistrate Judge's ultimate conclusions that the Motion to Suppress and the Motion for Evidentiary Hearing each should be denied (Dkt. #49). Defendant does not specifically object to the Magistrate Judge's findings that the Motion for Continuance should be denied as moot or that the NIT Warrant issued in violation of Rule 41(b) and § 636 (*see* Dkt. #49). As such, the Court adopts these findings and proceeds to evaluate Defendant's specific objections that (1) the Magistrate Judge erred in finding the NIT Warrant sufficiently particularized, (2) the Magistrate Judge improperly found a "technical" violation of Rule 41(b) and § 636 when the violation was instead of constitutional dimension, and (3) the Magistrate Judge erroneously concluded the good-faith exception applies (Dkt. #49).

Objection 1: NIT Warrant Particularity

Defendant first objects to the Magistrate Judge's conclusion that the NIT Warrant sufficiently particularizes the "place to be searched" (Dkt. #49 at 1-2). Specifically, Defendant argues "the description of the place to be searched 'activating computers' of users lacks sufficient particularity to pass constitutional muster" (Dkt. #49). Defendant asserts the search of Defendant's computer constitutes a "physically invasive inspection" that occurred in Defendant's home, and argues the United States Supreme Court's decision in *Berger v. State of N.Y.*, 388 U.S. 41 (1967), is analogous authority. The Government contends in response that the NIT was sufficiently particular given the description of the "place to be searched" in Attachment A (Dkt. #50 at 1-2). Further, the Government argues, Defendant's citation to *Berger* is inapposite and his argument

that the NIT Warrant authorized a "physically invasive search" mischaracterizes the NIT's function (Dkt. #50 at 2-3).

In *Berger*, the U.S. Supreme Court found a New York statute unconstitutional that permitted eavesdropping through a device installed in the target's office. *See* 388 U.S. at 45, 55-56. The *Berger* Court traced U.S. Supreme Court wiretap precedent and found that, generally, where the Government had accomplished its eavesdropping "without entry upon [the target's] premises[,]" the Government had not violated the Fourth Amendment, even where "devices ha[d] been used to enable government agents to overhear conversations which would have been beyond the reach of the human ear." *Id.* at 50-52. On the other hand, where that "eavesdropping was accomplished by means of an unauthorized physical penetration" of a "constitutionally protected area[,]" such eavesdropping was found unconstitutional. *Id.* The *Berger* Court then turned to the challenged New York statute, which permitted "a warrant [to] issue on reasonable ground to believe that evidence of a crime may be obtained by the eavesdrop." *Id.* at 55. The Court concluded that the statute "la[id] down no requirement for particularity in the warrant as to what specific crime has been or is being committed, nor 'the place to be searched,' or 'the persons or things to be seized' as specifically required by the Fourth Amendment" and accordingly found the statute unconstitutional. *Id.* at 55-56.

Berger is inapposite here for several reasons. First, *Berger* addressed the constitutionality of a statute permitting issuance of general warrants. Though the target of the statute had standing to challenge the statute because he suffered harm through a warrant issued thereunder, the Court focused its review on the statute, not the warrant itself. *See id.* at 64 (finding the statute as written facially invalid). Second, the NIT Warrant, through the incorporated Attachment A, authorized search only of computers whose users reached out to Website A's server. The Macfarlane

Affidavit (also incorporated by reference in the NIT Warrant) describes in detail the function of the NIT, computers generally, and the particular crimes related to possession, production, and distribution of child pornography that the NIT Warrant targets. Any *Berger* analogy accordingly fails because the NIT Warrant, unlike the statute at issue in *Berger*, makes clear "what specific crime has been or is being [allegedly] committed" ("Engaging in Child Exploitation Enterprise, Advertising and Conspiracy to Advertise Child Pornography; Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; Knowing Access or Attempted Access With Intent to View Child Pornography"), which place is "to be searched" (computers accessing Website A's server), and what "things" will "be seized" (the seven pieces of information described *supra*). The Court finds Defendant's objection based on *Berger* inapposite.

Furthermore, the Court agrees with the Magistrate Judge that the NIT Warrant sufficiently particularizes the place to be searched as "the activating computers through the NIT deployed on the Website A server" and that this description meets constitutional requirements (*see* Dkt. #47 at 11). The Magistrate Judge cites numerous courts throughout the country (including one in this circuit) in support of the conclusion that the NIT Warrant sufficiently particularizes the place to be searched in this manner (Dkt. #47 at 10). The Court in its own research has found the same. *See, e.g., United States v. Jean*, 207 F. Supp. 3d 920, 936 (W.D. Ark. 2016) ("The term 'activating computer' as used in the exhibits attached to and incorporated into the warrant has a specific meaning and context. The term refers to the computer of any Playpen user who subsequently logged into the website with a username and password. . . . As stated in the affidavit submitted in support of the warrant request, it is clear that users' 'activating computers' are understood to be accessing the website via the internet, and given the anonymity provided by the TOR browser, the users could be located anywhere in the world—which created the necessity of the NIT in the first

place. Thus, the context for what the FBI was seeking—and what the magistrate judge knowingly ordered by using this term in her warrant—was authority to search any 'activating computer'—'wherever located.'"); *United States v. Knowles*, 207 F. Supp. 3d 585, 602 (D.S.C. 2016) ("Here, the Government described the object into which the NIT was to be placed (user computers logging into Playpen), the circumstances that led agents to wish to install the NIT (users accessing child pornography on a hidden website, using advanced encryption tools impervious to normal investigative techniques), and the period of surveillance (the warrant application specified thirty days . . . , though the operation lasted only two weeks)."); *United States v. Hammond*, No. 16-CR-00102-JD-1, 2016 WL 7157762, at *3 (N.D. Cal. Dec. 8, 2016) ("Like the majority of courts looking at the issue, the Court finds that the NIT warrant was sufficiently particularized."); *United States v. Epich*, No. 15-CR-163-PP, 2016 WL 953269, at *2 (E.D. Wis. Mar. 14, 2016) ("[The NIT Warrant] explained who was subject to the search, what information the NIT would obtain, the time period during which the NIT would be used, and how it would be used, as well as bearing attachments describing the place to be searched and the information to be seized.").

Moreover, to the extent Defendant contends the NIT Warrant should have described the place to be searched as his home, the Court rejects such argument. As the court in *Knowles* noted:

> A search warrant seeking an address from any computer that deliberately logs into a hidden, illegal website hosted on a particular server is sufficiently particular, despite Defendant's argument that "[h]ad the government particularly described the place to be searched, *i.e.*, a computer in South Carolina, no warrant could have issued." . . . Defendant's argument is tendentious. The point of the NIT search warrant was to learn the location of computers accessing Playpen. If the Government knew Defendant's computer was in South Carolina, no NIT search warrant regarding this Defendant would have issued because the Government would not have needed one.

Knowles, 207 F. Supp. 3d at 602. The U.S. Supreme Court has held in the tracking device context that "describ[ing] the object into which the [device] is to be placed, the circumstances that led

agents to wish to install the [device], and the length of time for which [the device's] surveillance is requested . . . will suffice to permit issuance of a warrant authorizing [the device's] installation and surveillance." *United States v. Karo*, 468 U.S. 705, 718 (1984). The *Karo* Court found as much where "the location of the place [to be searched] [was] precisely what [was] sought to be discovered . . . ." *Id.* In light of *Karo*, even were the Court to conclude the "place to be searched" was Defendant's home—and the Court does not—the NIT Warrant would survive scrutiny. The NIT Warrant read in tandem with the Macfarlane Affidavit meets all of the *Karo* Court's criteria: it describes the Website A server and how the FBI came to possess it, it cites to the various statutes (proscribing possession, production, or distribution of child pornography) involved as well as the circumstances underlying the FBI's investigation of users of Website A, and it strictly limits the period in which the FBI could execute the warrant (*see* NIT Warrant; Macfarlane Affidavit at 2-4, 10-23). Accordingly, the Court overrules Defendant's first objection.

Objection 2: Effect of Rule 41(b) and § 636 Violation

Defendant also objects that the Magistrate Judge erroneously found the Rule 41(b) and § 636 violations "technical" rather than constitutional (Dkt. #49 at 2). Defendant contends the violations "are jurisdictional" and "make the issuance of the warrant void, since the [Eastern District of Virginia Magistrate] acted without authority, and thus stepped out of the role of being neutral and detached" (Dkt. #49 at 2). The Government argues in response that Defendant alters the arguments made before the Magistrate Judge by recasting the alleged jurisdictional violation as one implicating the Eastern District of Virginia Magistrate's neutrality; further, the Government contends Defendant cites no authority in support of such new argument (Dkt. #50 at 3-4). The Government argues that, in any event, the Magistrate Judge's conclusion that a "jurisdictional"

violation would not necessarily void the NIT Warrant is supported by reasoning and caselaw that Defendant's objection does not draw into question (Dkt. #50 at 4).

Indeed, Defendant's objection attacks the Magistrate Judge's conclusion, but does not address or attempt to distinguish the Magistrate Judge's reasoning (*see* Dkt. #47 at 16-18). The Magistrate Judge rests the conclusion that the violations do not merit suppression despite the jurisdictional nature of § 636, in part, on the premise that district courts in the Fifth Circuit have found that a violation of § 636 does not necessarily implicate a defendant's Fourth Amendment rights (Dkt. #47 at 17 (citing *United States v. Perdue*, No. 3:16-CR-305-D(1), 2017 WL 661378, at *4 (N.D. Tex. Feb. 17, 2017); *United States v. Pawlak*, No. 3:16-cr-306-D(1), 2017 WL 661371, at *6 (N.D. Tex. Feb. 17, 2017); *United States v. Torres*, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *7 (W.D. Tex. Sept. 9, 2016))). The authority the Magistrate Judge cites distinguishes between "the powers of magistrate judges"—i.e., their jurisdiction, which statutes govern—and their neutrality, which the Constitution guarantees. *Perdue*, 2017 WL 661378, at *4. The Magistrate Judge further expounded that suppression based on the instant violation of Rule 41(b) and/or § 636 would punish judicial error, rather than deter bad police conduct, which is the true aim of the exclusionary rule (Dkt. #47 at 17-18). Finally, the Magistrate Judge found that the ambiguity of Rule 41(b) as applied in the NIT context militates against concluding the violation amounts to a constitutional one (Dkt. #47 at 18). Defendant's objection touches specifically upon the first finding—that the Eastern District of Virginia Magistrate's issuing the NIT Warrant in violation of Rule 41(b) and § 636 does not implicate the Eastern District of Virginia Magistrate's neutrality (*see* Dkt. #49 at 2). Numerous courts have found that a Rule 41 and § 636 violation in issuance of a warrant does not implicate the issuing magistrate's neutrality. *See, e.g.*, *Perdue*, 2017 WL 661378, at *4; *United States v. Dorosheff*, No. 16-30049, 2017 WL 1532267, at *7 (C.D. Ill. Apr. 27, 2017) ("Nor does the Rule 41 violation indicate that the issuing judge was not 'detached and neutral.' There is no indication that the magistrate

deliberately violated Rule 41, nor that the officers misled the magistrate in their application."); *United States v. Henderson*, No. 15-CR-00565-WHO-1, 2016 WL 4549108, at *6 (N.D. Cal. Sept. 1, 2016) ("Here, the NIT Warrant was [*inter alia*] . . . issued by a neutral magistrate judge."); *Knowles*, 207 F. Supp. 3d at 601 (observing the Eastern District of Virginia Magistrate "was a neutral and detached judicial officer"). The Court finds likewise that the Rule 41(b) and § 636 violation did not impact the Eastern District of Virginia Magistrate's neutrality or otherwise indicate a lack of neutrality, given that Rule 41(b)'s applicability in the NIT context was unclear at the time the Eastern District of Virginia Magistrate issued the NIT Warrant and because the record contains no argument or evidence that the Eastern District of Virginia Magistrate was in any way biased. The Court overrules Defendant's second objection.

Objection 3: Good Faith Applicability and the Motion for Evidentiary Hearing

Defendant argues, as well, that the Magistrate Judge improperly found the good-faith exception applies without first conducting an evidentiary hearing to determine (1) whether "Mac[f]arlane mislead [sic] the [Eastern District of] Virginia Magistrate Judge in Attachment A of the warrant application in that it highlighted the placement of the NIT on the government controlled server and failed to disclose the physically invasive nature of the NIT searches"; (2) whether "Mac[f]arlane mislead [sic] the [Eastern District of Virginia] Magistrate Judge about the contents of the home page of [Website A]"; and (3) whether the Department of Justice ("DOJ") provided the FBI approval to seek the NIT Warrant "knowing Rule 41 did not authorize it" (Dkt. #49 at 2-3). The Government argues in response as follows: first, that Attachment A sufficiently identifies the place to be searched; second, that Defendant provides no support for his claim that Macfarlane misled the Eastern District of Virginia Magistrate about the contents of Website A; and third, that Defendant also provides no support for his claim that the FBI and/or

DOJ knew that Rule 41(b) could not support issuance of the NIT Warrant by the Eastern District of Virginia Magistrate (Dkt. #50 at 4-5).

"Under the good-faith exception, evidence obtained during the execution of a warrant later determined to be deficient is admissible nonetheless, so long as the executing officers' reliance on the warrant was objectively reasonable and in good faith." *United States v. Payne*, 341 F.3d 393, 399 (5th Cir. 2003) (citing *United States v. Leon*, 468 U.S. 897 (1984)). "The 'good faith inquiry is confined to the objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization.'" *United States v. Pope*, 467 F.3d 912, 916 (5th Cir. 2006) (quoting *Leon*, 568 U.S. at 922 n.23). Normally, the issuance of a warrant by a magistrate suffices to establish an officer's good faith. *United States v. Pena-Rodriquez*, 110 F.3d 1120, 1130 (5th Cir. 1997). But good faith cannot be established if one of the following four circumstances is present:

> (1) [i]f the issuing magistrate/judge was misled by information in an affidavit that the affiant knew was false or would have known except for reckless disregard of the truth; (2) where the issuing magistrate/judge wholly abandoned his or her judicial role; (3) where the warrant is based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) where the warrant is so facially deficient in failing to particularize the place to be searched or the things to be seized that the executing officers cannot reasonably presume it to be valid.

Payne, 341 F.3d at 399-400 (quoting *United States v. Webster*, 960 F.2d 1301, 1307 n.4 (5th Cir. 1992)) (hereinafter referred to as the "*Leon* exceptions"). Notably, in considering whether the good-faith exception applies, the Court does not attempt to determine the officers' subjective belief regarding the validity of the warrant. *See Leon*, 468 U.S. at 922 n.23. Rather, the Court's inquiry is "confined to the objectively ascertainable question of whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization." *Id.* Whenever a defendant seeks evidentiary hearing to further demonstrate some aspect of an

argument for suppression, such as the existence of a *Leon* exception, the defendant must "allege[] sufficient facts which, if proven, would justify relief." *United States v. Harrelson*, 705 F.2d 733, 737 (5th Cir. 1983). "[M]ere suspicion or conjecture[] will not suffice . . . ." *Id.*

Defendant seemingly contends the first *Leon* exception applies and that an evidentiary hearing would demonstrate as much (*see* Dkt. #49 at 2-3). The Court disagrees. First, Defendant's allegations that Macfarlane misled the Eastern District of Virginia Magistrate with Attachment A have merit only if considered alongside Defendant's theories that the "place to be searched" was Defendant's home and that the NIT's function on Defendant's computer constituted a "physically invasive" search (*see* Dkt. #47). The Court rejects the first theory *supra* in its analysis of Defendant's first objection and finds the second theory unpersuasive, as well. As the *Knowles* court observed, "the Government 'presented the [Eastern District of Virginia Magistrate] with all relevant information to allow her to make a decision as to whether Rule 41(b) permitted her to issue the [NIT Warrant]. The FBI agents did not misrepresent how the search would be conducted or, most importantly, where it would be conducted.'" 207 F. Supp. 3d at 603. The Court agrees with the Magistrate Judge that "Mac[f]arlane explained thoroughly to the Eastern District of Virginia Magistrate how the NIT would function and that . . . Mac[f]arlane expressly requested that the NIT Warrant authorize search of 'an activating computer—wherever located'" (Dkt. #47 at 23 (citing Macfarlane Affidavit at 23-27)). Attachment A expressly references such "activing computers" and the NIT in describing the "[p]lace to be searched."

Further, any allegation that Macfarlane misled the Eastern District of Virginia Magistrate about the content on Website A's homepage also would not establish Defendant's right to an evidentiary hearing. Macfarlane's Affidavit describes the home page of Website A as follows:

> On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." . . . Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' (a hyperlink to the registration page) with [TARGET WEBSITE name]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

(Macfarlane Affidavit at 13). The Affidavit then continues for seven more pages in describing Website A's content, referencing forums like "Jailbait – Boy" and "Preteen – Girl" and topic posts like "Sammy[,]" which "contained hundreds of images depicting" a prepubescent female sexually (Macfarlane Affidavit at 14-20). Defendant seemingly contends Macfarlane's description of the Website A homepage contains inaccuracies (*see* Dkt. #49 at 3). Arguments like Defendant's regarding the Macfarlane Affidavit's description of Website A's homepage have failed in light of the Macfarlane Affidavit's description of the remainder of Website A and Website A's hidden nature:

> Regardless of whether the technical language on the homepage and the site's location on the Tor network indicated criminality, it stands to reason that the casual accidental visitor probably would not locate the Playpen site on the Tor network, let alone create a username and password in order to log into the site, without having any idea as to what the site contained. The fact is that Playpen did contain child pornography, and the affiant knew it contained child pornography. Playpen's content, not its homepage, was the necessary factor in the probable cause determination. . . . There is at least a reasonable probability that evidence of a crime related to child pornography will be found on a computer that one uses to register with a website that displays child pornography, regardless of whether the homepage alone makes it obvious that the site is a child pornography site. . . . Therefore, while the information and image found on the homepage buttressed the conclusion that Playpen was a child pornography site, they were not essential to that conclusion.

United States v. McLamb, No. 2:16CR92, 2016 WL 6963046, at *4 (E.D. Va. Nov. 28, 2016); *see also United States v. Darby*, 190 F. Supp. 3d 520, 532 (E.D. Va. 2016) ("Furthermore, the homepage and logon process of Playpen are not the only basis for finding that the warrant was

supported by probable cause. The warrant application contains detailed information about the illegal content available on the Playpen website."); *Jean*, 207 F. Supp. 3d at 934 (concluding the detailed Macfarlane Affidavit clearly demonstrates the explicit, illegal nature of Website A's content notwithstanding its description of the homepage). And courts have generally denied requests for evidentiary hearing on this point. *See, e.g.*, *United States v. Matish*, 193 F. Supp. 3d 585, 605-06 (E.D. Va. 2016) (denying defendant's request for evidentiary hearing on this matter); *United States v. Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *1 (W.D. Wash. Jan. 28, 2016) (same); *Pawlak*, 2017 WL 661371, at *1 n.2 (denying FBI testimony as "unnecessary for [the court's] analysis of the good-faith exception"). Moreover, Defendant admits the alleged inaccuracies in describing the homepage "may be de minimis" (Dkt. #46 at 7).

Finally, the Court agrees with the Magistrate Judge that the DOJ's and/or FBI's subjective beliefs about whether Rule 41(b) authorized a magistrate judge to issue the NIT Warrant does not impact the good-faith exception analysis. As noted, "[t]he 'good faith inquiry is confined to the objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization.'" *Pope*, 467 F.3d at 916. Bringing Macfarlane into court to answer questions about what Macfarlane or the DOJ attorney(s) with whom he spoke believed regarding the legality of the NIT Warrant would not answer the central question, namely what the objective, "reasonably well-trained officer would have known" about Rule 41(b)'s reach at the time. *See, e.g.*, *United States v. Ammons*, 207 F. Supp. 3d 732 (W.D. Ky. 2016) (denying without evidentiary hearing defendant's motion to suppress by applying good-faith exception); *Michaud*, 2016 WL 337263 (same); *United States v. Gaver*, No. 3:16-cr-88, 2017 WL 1134814 (S.D. Ohio Mar. 27, 2017) (denying defendant's request for evidentiary hearing); *Pawlak*, 2017 WL 661371, at *1 n.2 (same). The very fact that courts have split on the

question of whether Rule 41(b) authorized the Eastern District of Virginia Magistrate to issue the NIT Warrant demonstrates that a reasonably well-trained officer could have concluded the NIT Warrant issued lawfully. *See, e.g.*, *United States v. Acevedo-Lemus*, No. SACR 15-00137-CJC, 2016 WL 4208436, at *7 (C.D. Cal. Aug. 8, 2016) ("As an initial matter, there are credible arguments to be made that Rule 41 was never violated at all, casting doubt on Defendant's assertion that the FBI was knowingly flouting the Rule."); *Matish*, 2016 WL 3545776, at *18 ("[T]he NIT Warrant authorized the FBI to install a tracking device on each user's computer when that computer entered the Eastern District of Virginia . . . [w]hen that computer left Virginia—when the user logged out of Playpen—the NIT worked to determine its location . . . all relevant events occurred in Virginia."); *see also Knowles*, 207 F. Supp. 3d at 603 (citing *Darby* to show that courts considering the NIT Warrant even after the fact have found it complied with Rule 41); *cf. Darby*, 190 F. Supp. 3d at 536 (holding that Rule 41(b)(4) authorized the NIT Warrant); *Dorosheff*, 2017 WL 1532267, at *7. Additionally, and as the Magistrate Judge noted, refusing to apply the good-faith exception in this case would punish judicial error, not police misconduct. *See, e.g.*, *Dorosheff*, 2017 WL 1532267, at *7 ("Further, because nothing before the Court indicates that the executing officers did not act in good faith reliance on the validity of the warrant or that they acted culpably or deliberately in violating Rule 41, suppression is not warranted because it would not deter police misconduct and it would remove relevant and reliable evidence from the public."); *Jean*, 207 F. Supp. 3d at 945 ("There is simply no indication that law enforcement suspected the warrant was lacking in probable cause or sufficient particularity, or that agents believed the magistrate judge might lack the jurisdictional authority to authorize the relatively new technology described in the warrant application."); *Henderson*, 2016 WL 4549108, at *5-6 (finding good-faith exception applies). The Court concludes the good-faith exception applies here and that it needs no further

evidence to make such determination. The Court accordingly overrules Defendant's third objection.

CONCLUSION

Having received the report of the Magistrate Judge (Dkt. #47), having considered each of Defendant's objections (Dkt. #49) and the Government's Response (Dkt. #50), and having conducted a de novo review, the Court is of the opinion that the Magistrate Judge's recommendation that Defendant's Motion to Suppress Evidence (Dkt. #25), Motion for Continuance of Suppression Hearing (Dkt. #40), and Opposed Motion Requesting Evidentiary Hearing (Dkt. #41) each be denied is correct.

It is, therefore, **ORDERED** that Motion to Suppress Evidence (Dkt. #25), Motion for Continuance of Suppression Hearing (Dkt. #40), and Opposed Motion Requesting Evidentiary Hearing (Dkt. #41) each are **DENIED**.

IT IS SO ORDERED.

SIGNED this 26th day of May, 2017.

AMOS L. MAZZANT
UNITED STATES DISTRICT JUDGE